

SOC 2

(System and Organization Controls 2)

Compliance

Checklist



Introduction

What is SOC 2?

ISO 27001 is a globally recognized standard that outlines how to build, operate, maintain, and improve an Information Security Management System (ISMS). An ISMS is a structured framework designed to keep sensitive business information secure by integrating people, processes, and technology.

Where is SOC 2 Used?

SOC 2 is most commonly required by:

- Cloud service providers (SaaS, IaaS, PaaS)
- B2B companies handling client or user data
- Managed service providers, data processors, and IT consultants
- Organizations pursuing enterprise clients, especially in regulated sectors

SOC 2 is increasingly becoming a requirement for organizations aiming to demonstrate compliance with industry regulations like GDPR or HIPAA.

Many enterprises now require SOC 2 reports from vendors as part of their security review process.

How Does SOC 2 Work?

SOC 2 compliance involves creating and maintaining controls that meet one or more of the five Trust Services Criteria:

- Security (mandatory)
- Availability
- Processing Integrity
- Confidentiality
- Privacy

The compliance process typically involves:

- Scoping your systems and criteria
- Designing internal policies, security measures, and monitoring systems
- Working with an external auditor (CPA (Certified Public Accountant) firm)
- Maintaining evidence and documentation over time

A Type I report focuses on the design of controls at a specific point in time, while a Type II report assesses the operating effectiveness of these controls over a defined period (usually 6 to 12 months).

This checklist will guide your team through the core requirements and best practices necessary for SOC 2 readiness and ongoing compliance.

Category 1: Define Scope and Objectives

Sub-category	Checklist Item/Control	Description/Details	Status
Scoping	Identified the systems/services that processed or stored client data	All SaaS platforms, internal servers, and databases handling customer PII.	☐
Criteria Selection	Determined which Trust Services Criteria applied: Security, Availability, Confidentiality	Based on service offerings and client expectations.	☐
Report Type	Determine whether a Type I or Type II report is needed	Based on maturity, audit goals, and client expectations	☐
CPA Firm	Choose a CPA firm with experience in IT/Security Audits	Must be AICPA-licensed and SOC 2 experienced	☐
Subservice Organizations Mapping	Map third-party relationships and define Subservice Controls (CSOCs)	Document shared vs. carved-out controls	☐
CUECs (Client User Entity Controls)	Document Customer-side controls (CUECs) based on dependencies	Based on shared responsibility with clients	☐

Category 2: Security (Common Criteria)

Organizational Controls	Maintain an approved, annually reviewed security policy	Ensure documented policies are reviewed and approved annually.	☐
	Define and assign security roles and responsibilities	Establish accountability for security functions across teams.	☐
Access Controls	Apply Role-Based Access Control and least privilege	Ensure users only access what's needed for their roles.	☐
	Provision and de-provision user access promptly	Manage lifecycle access processes for all users.	☐
	Conduct routine access reviews	Review access rights quarterly or as needed.	☐
	Provision and de-provision user access promptly	Manage lifecycle access processes for all users.	☐
System Operations and Monitoring	Implement centralized logging and SIEM monitoring	Enable logs and monitor using SIEM tools for anomalies.	☐
	Run vulnerability scans and risk assessments regularly	Perform scanning and analysis to detect system weaknesses.	☐
	Maintain and test an incident response plan	Ensure team readiness and plan effectiveness.	☐
	Deploy anti-malware and endpoint protection	Use up-to-date endpoint security tools.	☐

Change Management	Implement formal change approval workflows	Track and approve changes systematically.	☐
	Segregate development and production environments	Avoid unapproved code or access leaks between environments.	☐
	Test and document all changes before deployment	Document test results and change logs.	☐
Risk Management	Conduct annual risk assessments	Identify and document business and technical risks.	☐
	Maintain an active risk treatment plan	Define mitigation strategies for known risks.	☐

Category 3: Availability (If in Scope)

SLAs	Define SLAs and uptime targets	Establish availability metrics and monitor adherence.	☐
Capacity Planning	Assess system capacity regularly	Review performance and scale infrastructure as needed.	☐
Disaster Recovery	Test backup and disaster recovery plans annually	Verify recovery processes and backup data integrity.	☐
Incident Management	Document incident escalation paths	Ensure staff know how to escalate issues appropriately.	☐

Category 4: Processing Integrity (If in Scope)

Validation	Validate data inputs and outputs	Ensure systems accurately process and transfer data.	☐
Monitoring	Log and review processing workflows	Monitor workflow execution and data flows.	☐
Error Handling	Identify and resolve processing errors promptly	Track, log, and resolve any integrity-related issues.	☐
Transaction Completeness	Ensure transactions are complete and accurate	Check for missing, partial, or incorrect transactions.	☐

Category 5: Confidentiality (If in Scope)

Data Classification	Implement a classification and labeling policy	Define data types and label them by sensitivity.	☐
Encryption	Encrypt confidential data at rest and in transit	Use strong encryption standards like AES-256, TLS.	☐
NDA's	Require NDAs for access to sensitive data	Apply to employees, vendors, contractors.	☐
Secure Disposal	Follow media and data disposal procedures	Wipe, shred, or destroy storage as per policy.	☐

Category 6: Privacy (If in Scope)

Privacy Notice	Publish a transparent privacy notice	Reflect actual practices in the notice published.	☐
Consent Management	Implement user consent mechanisms	Ask users to opt-in for data collection or use.	☐
User Rights	Support data access, correction, and deletion	Enable users to request changes or removal.	☐
Retention Policy	Maintain and apply a data retention schedule	Purge data as per legal or business policy.	☐

Category 7: Vendor Management

Risk Assessment	Perform vendor risk assessments	Assess vendor data handling and security posture.	☐
Assurance	Collect SOC 2 or equivalent reports	Obtain ISO/SOC reports from critical vendors.	☐
Contract Clauses	Include security and privacy clauses in contracts	Add breach notification and control requirements.	☐
Ongoing Review	Schedule regular vendor evaluations	Review contracts and re-assess risk annually.	☐

Category 8: Audit Readiness and Documentation

Policy Management	Version-control and maintain access to all policies	Track changes and document ownership.	☐
Evidence Collection	Organize logs and evidence in advance	Maintain a centralized repository of proof.	☐
Control Ownership	Assign and train control owners	Define who manages each control item.	☐
Readiness Assessment	Conduct a gap analysis or internal audit	Identify and address non-compliance areas.	☐

Category 9: Ongoing Compliance

Self-Assessments	Perform quarterly control reviews	Review and update control status regularly.	☐
Annual Review	Conduct annual internal or external audit	Plan and document review findings.	☐
Training	Provide security and privacy training annually	Train all staff annually on evolving security threats and update policies to reflect any changes in technology or legal requirements.	☐
Policy Updates	Update policies with tech and legal changes	Purge data as per legal or business policy.	☐



Found this **useful?**

Get More Insights Through our **FREE**

Courses | Webinars | eBooks | Whitepapers | Checklists | Mock Tests



www.infosectrain.com